UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/618,861	07/14/2003	Eric Balard	TI-34921	6971

23494 7590 06/18/2008

TEXAS INSTRUMENTS INCORPORATED
P O BOX 655474, M/S 3999
DALLAS, TX 75265

EXAMINER	
LANIER, BENJAMIN E	

ART UNIT	PAPER NUMBER
2132	

NOTIFICATION DATE	DELIVERY MODE
06/18/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspto@ti.com
uspto@dlemail.itg.ti.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/618,861
Filing Date: July 14, 2003
Appellant(s): BALARD ET AL.

Ronald O. Neerings
Reg. No. 34,227
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 02 May 2007 appealing from the Office action mailed 01 November 2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,268,788	GRAY	7-2001
5,768,373	LOHSTROH	6-1998
6,314,521	DEBRY	11-2001
6,824,051	REDDY	11-2004

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1, 4-7, 10-13, 15-21, 23-24, 26-28, 30, 33-38, 40, 41, 43-45 are rejected under 35 U.S.C. 102(e) as being anticipated by Gray, US patent, 6268788.

In reference to claim 1:

Gray (Column 5, lines 62- Column 6, lines 20) & (Column 6, lines 55-Column 7, line 10) & Figure 4 discloses a method of securing access to resources in a computing device, comprising the steps of:

- Storing an encrypted access code in a memory location within the computing device; (Figure 2 & Column 5, lines 62- Column 6, lines 20) & (Column 6, lines 55-Column 7, line 10)
- Receiving a password to access the resources; (Column 5, lines 62- Column 6, lines 20) & (Column 6, lines 55-Column 7, line 10)
- Encrypting the password to produce the encrypted access code; (Column 5, lines 62-Column 6, lines 20) & (Column 6, lines 55-Column 7, line 10)
- Allowing access to the resources if the encrypted access code matches the encrypted password. (Column 6, lines 16-20) & (Column 6, line 65- Column 7, line 5)

In reference to claim 4:

Gray (Column 5, lines 62- Column 6, lines 20) & (Column 9, lines 53-65) discloses the method of claim 1 wherein the encrypted access code is stored in a memory that cannot be externally modified, where the information stored on the computer system cannot be captured or tampered with and is stored in a secure room.

In reference to claim 5:

Gray (Column 6, lines 55-Column 7, line 10) discloses the method of claim 1 wherein the step of allowing access comprises the step of allowing access to testing resources if the encrypted access code matches the encrypted password.

In reference to claim 6:

Gray (Column 6, lines 55-Column 7, line 10) discloses the method of claim 1 wherein the step of allowing access comprises the step of allowing access to change system parameters if the encrypted access code matches the encrypted password.

In reference to claim 7:

Gray (Column 5, lines 62- Column 6, lines 20) & (Column 6, lines 55-Column 7, line 10) & Figures 2, 4 discloses a computing device comprising:

- A processing system (Figure 2, Items 40 and Items 60)

- A memory coupled to the processing system for storing an encrypted access code; (Figure 2, Items 42 and Items 62)
- Input circuitry coupled to the processing system for receiving a password to access resources; (Figure 2, Items 16 and Items 34)
- Wherein the processing circuitry:
    - Encrypts the password to produce a encrypted password; (Column 6, lines 1-8) & (Column 6, lines 55-Column 7, line 10)
    - Compares the encrypted password to the encrypted access code; (Column 6, lines 1-8) & (Column 6, lines 55-Column 7, line 10)
    - Allows access to the resources if the encrypted access code matches the encrypted (Column 6, lines 55-Column 7, line 10)

In reference to claim 10:

Gray (Column 5, lines 62- Column 6, lines 20) & (Column 9, lines 53-65) discloses the computing device of claim 7 wherein the encrypted access code is stored in a memory that cannot be externally modified, where the information stored on the computer system cannot be captured or tampered with and is stored in a secure room.

In reference to claim 11:

Gray (Column 6, lines 55-Column 7, line 10) discloses the computing device of claim 7 wherein the processing system allows access to testing resources if the encrypted access code matches the encrypted password.

In reference to claim 12:

Gray (Column 6, lines 55-Column 7, line 10) discloses the computing device of claim 7 wherein the processing system allows access to system parameters if the encrypted access code matches the encrypted password.

In reference to claims 13, 15, 30:

Gray discloses that the authenticating system (Figure 2, element 10) meets the limitation of the claimed "computing device". Furthermore, when considering the disclosure of Gray it is clear that the computer 12 and the verification unit 20 make up a singular device for the simple reason that the verification unit 12 draws its power from the computer 12 (Col. 4, lines 15-20), which meets the limitation of the memory location is within a processing system in the computing device, the memory location is in a memory subsystem within the processing system. Therefore, without the computer 12, the verification unit 12 cannot operate and therefore cannot be considered a "device" on its own.

In reference to claims 16-18, 33-35:

Gray discloses that the memory can include a ROM (Figure 2, 64), which meets the limitation of the memory subsystem comprises a memory array in which after data is written to the array,

further writing to the particular memory location is disabled, such that the data cannot be overwritten, a read only memory (ROM) coupled to the memory array, some portions of the memory array are externally accessible but not modifiable.

In reference to claims 19, 36:

Gray discloses that memory could be password protected (Col. 9, lines 21-28), which meets the limitation of wherein some portions or the memory array are not externally accessible and are not modifiable.

In reference to claims 20, 37:

Gray discloses that encryption keys are stored in memory (Col. 11, lines 54-56), which meets the limitation of an encryption key is stored in the memory array.

In reference to claims 21, 38:

Gray discloses that the encryption keys are generated using random numbers in the verification unit (Col. 12, lines 6-13), which meets the limitation of the encryption key is generated by a random number generator internal to the processing system.

In reference to claims 23, 40:

Gray discloses at least one processor coupled to the memory subsystem (Figure 2).

In reference to claims 24, 41:

Gray discloses a non-volatile memory system coupled to the processing system wherein the non-volatile memory system is external to the processing system internal to the computing system (Figure 2).

In reference to claims 26, 43:

Gray discloses that the memory stores an encrypted PIN for comparison (Col. 6, lines 55-60), which meets the limitation of a test ID stored in the array.

In reference to claims 27, 28, 44, 45:

Gray discloses that the verification unit provides cryptographic capabilities (Col. 6, lines 55-57), which meets the limitation of the read only memory (ROM) further comprises cryptographic software, the non-volatile memory system includes application software, data files.

Claims 2, 3, 8, 9, 29, 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gray and Lohstroh et al, US patent 5768373.

In reference to claims 2, 3, 8, 9, 29, 46:

Gray fails to explicitly disclose the method of claim 1 wherein the step of storing an encrypted access code comprises the step of storing a hashed access code.

Lohstroh, paragraph 15 teaches

(15) The encryption/decryption algorithm performed by units 252 and 258 is symmetric. Thus, since K.sub.acc is supplied to encryption unit 252, K.sub.acc

*must also be supplied to decryption unit 258. Yet, as with other keys, if K.sub.acc is stored in plaintext form in non-volatile storage means, and sometime later an unauthorized person discovers the location of K.sub.acc, the security of data will be compromised as other encrypted keys will then become accessible. Therefore, access key K.sub.acc is supplied on line 232 to encrypting unit 234 which operates according to well-known symmetric encryption/decryption algorithms such as "Blowfish", which can generally be found in Bruce Schneier, Applied Cryptography (2d.Ed. 1995). The resulting encrypted signal *K.sub.acc:1 * produced on line 236 is stored in storage region 238. The key signal that is applied to encrypting unit 234 on line 264 is K.sub.pwh and is produced by hashing unit 262 from a user-supplied password on line 261. "Hashing" is generally the using of an algorithm to take a variable size input and produce a unique fixed-length identifier representative of the original input (here, the user password). One hash algorithm, MD5, or message digest 5, is generally known in the art, and is suitable for hashing a user password. Other algorithms are also generally known and are also suitable for hashing a user password in accordance with the invention. Often hash functions are thought to take a large block of data and reduce it to a smaller block. However, because the user password can vary from a few characters to up to 99 bytes in one embodiment, hash function 262 may produce a larger or smaller block of data than a given input (the user password), but it will return a password hash (K.sub.pwh) of consistently fixed length. In one embodiment*

using the MD5 hash function, such fixed length is set to 16 bytes.

Thus Lohstroh teaches an embodiment where an access key or "access code" is encrypted by first hashing it.

"The key signal that is applied to encrypting unit 234 on line 264 is K.sub.pwh and is produced by hashing unit 262 from a user-supplied password on line 261."

Lohstroh also teaches that the password can vary from a few characters up to 99 bytes, but after the hash, it will return a password hash of consistently fixed length.

It would have been obvious to one of ordinary skill in the art at the time of invention to use a hash as a step in a cryptographic process to encrypt the hash in order to reduce a variable length password into a fixed length, providing for greater password security by masking the length of and number of characters within the password.

Claims 14, 25, 31, 32, 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gray, U.S. Patent No. 6,268,788, in view of Reddy, U.S. Patent No. 6,824,051. Referring to claims 14, 25, 31, 32, 42, Gray discloses that the system shown in Figure 2 (element 10) is a traditional computer or workstation (Col. 4, lines 13-15). Gray does not disclose that the system is a mobile system such as a PDA, which utilizes baseband/rf technology. However, it would

have been obvious to provide the access control system described in Gray in a PDA embodiment because Gray discloses that there is an increased need to provide protection to sensitive information stored within computers systems (Col. 1, lines 19-37) and Reddy shows that PDAs are a reasonable form of computer system (Col. 6, lines 25-33).

Claims 22, 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gray, U.S. Patent No. 6,268,788, in view of Debry, U.S. Patent No. 6,314,521. Referring to claims 22, 39, Gray does not disclose that the encryption key is generated and stored at the time of manufacture. Debry discloses a device that stores an encryption key that was generated and stored at manufacture (Abstract). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the encryption key of Gray to be stored in the system at the time of manufacture in order for the encryption key to be stored in a tamper proof manner as taught by Debry (Col. 8, lines 18-28).

(10) Response to Argument

Appellant argues, "Examiner, however, now equates Gray's verification unit 20 with 'computing device' of claims 1 and 7." This argument is not persuasive because the Examiner clearly stated in the previous Office Action (See paragraph 2) that the authenticating system (Gray: Figure 2, element 10) met the limitation of the claimed "computing device." Examiner believes that majority of Appellant's arguments are made utilizing the misinterpretation of the previous rejection in view of Gray.

Appellant argues, "To the extent verification unit 20 has memory, it is not used to store any access code (much less an encrypted access code)." This argument is not persuasive because

"card 34" is an actual smartcard connected to the verification unit 20 via a PCMCIA card slot (Col. 4, lines 22-24). Therefore, the smartcard itself is a memory within the verification unit 20. Also, the encrypted password stored within the smartcard is additionally stored in the RAM 66 of the verification unit 20 prior to comparison with the entered password (Col. 7, lines 50-54). Therefore, Gray meets the claim limitation for at least two different reasons.

Appellant argues, "it is the card 34 that issues a 'pass' or a 'fail' signal via verification unit 20 to the computer 12, which either grants or denies execution control of application software to the operation." This argument is not persuasive because the processor 60 of the verification unit 20 determines if the entered encrypted password is valid by comparing it to the encrypted password previously stored on the card 34 (Col. 7, lines 54-58), and the result is sent to the computer 12 (Col. 7, lines 58-59). Gray clearly meets the limitation in question because within the authenticating system (Figure 2, 10), and encrypted access code is stored in a memory (Figure 2, 66 & 34) location within the authenticating system that is coupled a processing system (Figure 2, 60).

Appellant argues, "card 34 is a peripheral device that is NOT part of verification unit 20." This argument is not persuasive because the card 34 has a housing within the verification unit (Figure 2, 68), and therefore, when the card is inserted into the reader, the card is effectively a part of the verification unit in the same manner as the RAM or the ROM is part of the verification unit. The fact that the card may be easier to remove than the RAM or the ROM has no bearing on the fact that when inserted into the card reader, the card is part of the verification unit.

Appellant argues, "verification unit 20 does not authorize access to resources within verification unit 20 – it only compares passwords, with card 34 issuing a 'pass' or a 'fail' signal via the verification unit to the computer 12, which either grants or denies execution control of application software to the operator." This argument is not persuasive because since the authenticating system 10 reads on the claimed "computing system", access is being provided to software within the "computing device" because the computer 12 is within the authenticating system 10.

Appellant argues, "Gray does not teach…that its memories CANNOT be externally modified." This argument is not persuasive because Gray discloses that the card used to store the encrypted password can be **permanently** disabled (Col. 8, lines 13-16). One skilled in the art would understand that if the card 34 is permanently disabled, it cannot be modified.

Appellant argues that Gray does not teach "allowing access to testing resources if the encrypted access code matches the encrypted password." This argument is not persuasive because Gray discloses that the application software accessed by the user upon authentication can include local security programs (Col. 4, lines 52-53).

Appellant argues, "while the operator may access and/or alter the application program(s) unlocked through use of the password, (Col. 7, lines 5-7), Gray does not teach or suggest that a user will be able to change system parameters, as suggested by Examiner." This argument is not persuasive, because alteration of application programs effectively changes "parameters" associated with that application program. Therefore, Gray meets the limitation because the "system parameters" associated with the altered application program, have been effectively

altered. Appellant has not claimed changing any specific "system parameters" and therefore, Gray meets the limitation using a broad but reasonable interpretation.

Appellant argues, "Gray clearly shows in Fig. 2 that ROM 64 and RAM 66, are part of a memory module 62, which is separate from processor 60." In response, the Examiner would like to point out that claim 13 requires that "the memory location is within a **processing system** in the computing device. There is no claimed requirement for the claimed memory location to be within an actual processor as discussed by Appellant. In Gray, ROM 64, RAM 66, and card 34 are part of the verification unit 20, which includes a processor 60 and is therefore a processing system as claimed.

Appellant argues on page 9 of the Brief (first full paragraph) that the verification unit 20 and the computer 12 cannot be considered "a device" because "computer 12 does not need verification unit 20 to operate." This argument is not persuasive because Appellant appears to be utilizing their own definition of the term device. *The American Heritage Dictionary* defines "device" as simply "A contrivance or **an invention** serving a particular purpose, especially a machine used to **perform one or more relatively simple tasks**." In the case of Gray, it is clear that using the broad but reasonable interpretation of "device" the authentication system 10 of Gray can be considered a device since it represents a particular invention used to serve a particular purpose (i.e. authenticating access to software and utilization of software) by performing one or more relatively simple tasks. Appellant's arguments appear to suggest that authentication system 10 of Gray cannot be considered "a device" because all the elements of the authentication system 10 are not "mandatory parts of the processing system." Examiner is completely unaware of such a requirement. Nonetheless, the verification unit 20 of Gray is vital

to the operation of the of authentication system 10 since it actually performs the comparison used for authentication (Gray: Col. 7, lines 35-67).

Appellant's argument with respect to claim 15 mirrors the argument made with respect to claim 13, which was previously addressed above.

Appellant argues, "Gray, on the other hand, includes both ROM 64 and RAM 66 in its memory module 62. **While it may not be possible to write to ROM 64** it would be possible to write to RAM 66." In response, Gray discloses that the card used to store the encrypted password can be **permanently** disabled (Col. 8, lines 13-16). One skilled in the art would understand that if the card 34 is permanently disabled, it cannot be modified.

Appellant argues, "in Gray, ROM 64 and RAM 66 are the memory array in verification unit 20 – they are not 'coupled to a memory array'." This argument is not persuasive because ROM 64 and RAM 66 are clearly coupled to the memory 36 of the card 34 (See Figure 2).

Appellant argues, "Gray fails to teach or suggest, 'wherein some portions of the memory array **are not externally accessible and are not modifiable**', as required by claim 19." In response, Gray discloses that the card used to store the encrypted password can be **permanently** disabled (Col. 8, lines 13-16). One skilled in the art would understand that if the card 34 is permanently disabled, it cannot be modified.

Appellant's argument with respect to claim 20 is not persuasive because Gray discloses that the card 34 stores encryption keys (Col. 12, lines 15-23).

Appellant's argument with respect to claim 21 is not persuasive because Gray clearly discloses that the encryption keys are randomly generated (Col. 12, lines 15-23). Additionally the

entire authenticating system 10 can be considered and processing system and would therefore have had the random numbers generated within the authenticating system.

Appellant's argument with respect to claim 24 is not persuasive because Gray clearly shows (Figure 2) memory coupled to a processing system internal to the computing device.

Appellant argues, "Gray, however, fails to further teach or suggest, 'at least one of the following stored in the array: a test ID, a manufacturer's public key; a die identification number', as further required by claim 26." This argument is not persuasive because Gray discloses that the card 34 stores an encrypted personal identification number (Col. 6, lines 57-58), which meets the limitation of a test ID.

Appellant's argument with respect to claim 10 mirrors previous arguments that have already been addressed above.

Appellant's argument with respect to claim 11 mirrors previous arguments that have already been addressed above.

Appellant's argument with respect to claim 12 mirrors previous arguments that have already been addressed above.

Appellant's arguments with respect to claim 30 mirror previous arguments that have already been addressed above.

Appellant's argument with respect to claim 33 mirrors previous arguments that have already been addressed above.

Appellant's argument with respect to claim 34 mirrors previous arguments that have already been addressed above.

Appellant's argument with respect to claim 36 mirrors previous arguments that have already been addressed above.

Appellant's argument with respect to claim 37 mirrors previous arguments that have already been addressed above.

Appellant's argument with respect to claim 38 mirrors previous arguments that have already been addressed above.

Appellant's argument with respect to claim 41 mirrors previous arguments that have already been addressed above.

Appellant's argument with respect to claim 43 mirrors previous arguments that have already been addressed above.

Appellant's arguments with respect to the rejections made over Gray in view of Lohstroh, do not set forth any believed deficiencies that have not already been thoroughly addressed above.

Appellant's arguments with respect to the rejections made over Gray in view of Reddy, do not set forth any believed deficiencies that have not already been thoroughly addressed above.

Appellant's arguments with respect to the rejections made over Gray in view of Debry, do not set forth any believed deficiencies that have not already been thoroughly addressed above.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Benjamin E Lanier/
Primary Examiner, Art Unit 2132

Conferees:

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132

/Jung Kim/
Patent Examiner, Art Unit 2132